International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Double Encryption and Key Aggregation on Virtual Cloud

Shivraj Godle*, Sandip Kakade, Kundan Ithape, Sushil Giri

Department of Computer Engineering, Pune University/SAE Kondhawa/Pune, Maharashtra, India

ABSTRACT

Cloud computing is one of the fastest growing internet based technology that gives users to utilize services by making use of large poll of resources without installation of any software. Adoption of this technology is increasing rapidly because of many advantages including reduction of cost and IT load. In the double encryption and key aggregation on virtual cloud there is two method we will implement that are double encryption and key aggregation. Double encryption is the process in which we have to implement the process, which can encrypt the file at the time of uploading. After that when we have to download it will decrypt automatically by system with OTD. Despite the popularity of cloud computing, it faces many difficulties such as security that is one of the major inhibitors in the growth of cloud computing. Data confidentiality is at the top of the list of security concern for this technology. Here in this project we have another concept that is key aggregation, in that any user can send request for multiple file and user will allow access. Then User can download the file throw otd comes throw message on mobile. In the key aggregation, multiple keys for various file can be aggregated and user will get the OTD for one time download.

Keywords: Encryption, Cloud Computing, Key Generation, Decryption

I. INTRODUCTION

Cloud users store their data in encrypted form to maintain data privacy. Two approaches that are used to securely share data in cloud storage. Firstly, encrypt data using a symmetric key and share that key among the authorized users. Secondly, encrypt data using the individual public key of the authorized users. Authorized users can access plaintexts data by decrypting the corresponding cipher texts using their respective private key. However, the former approach incurs heavy overheads on the data owner, while storage overhead is more in the later [1]. Further, fine-grained access control in data sharing cannot be achieved from these two approaches [1]. To these issues, ABE [1]–[3] has emerged as a good alternative to achieve scalable fine-grained access control while sharing encrypted data among a set of authorized users in cloud environment [4], [5]. It allows data owners to encrypt data using an access policy of different attributes. The users who have sufficient attributes can decrypt the cipher texts. Although ABE schemes provide fine-grained access control in sharing data among a set of authorized users, revocation is remained challenging task [6], [7]. In ABE, more than one user may have same attributes. Therefore, user revocation should be done so that revoked users must not be able to access plaintexts data, while non-revoked authorized users should be able access plaintexts data without any difficulty. To the best of our knowledge, there are two approaches for achieving user revocation in ABE systems.

II. LITERATURE REVIEW

In cloud storage, user stores their data in encrypted form to prevent unauthorized access to data. In Section I, two common approaches to share encrypted data among a set of authorized users is discussed. However, these two approaches have limitations. In the symmetric key encryption approach, if a user is revoked from the system, the cipher texts need to be encrypted once again using a new symmetric key. The new symmetric key needs to be distributed among the non-revoked authorized users. Therefore, it is not an efficient scheme to use in data sharing if frequent user revocations occur. While the public key encryption encrypts same data using the individual public keys of the authorized users. Thus, it increases unnecessary storage overheads on the cloud storage servers. ABE has provided a suitable platform to achieve fine-grained access control for encrypted data in cloud environment.

The first cipher text-policy based ABE (CP-ABE) scheme was proposed by Bettencourt et.al. [3], where access policy is embedded in the cipher text itself. Thus encrypted can choose who can access data by embedding the access policies in the cipher texts which makes it suitable for data sharing in cloud environment. In later years many improved CP-ABE schemes have been proposed, for example [6], [8]– [10]. To solve the problem of user revocation in ABE systems first introduced expiration time based user revocation scheme [11]. After that many researchers have proposed their user revocation schemes . In the owner based revocation schemes [5], [6], [15], data owner handles revocation of the user.

A. PROPOSED SYSTEM

In the proposed system we have to implement the double encryption and key aggregation on virtual cloud. Here we use the cloud where we upload the files to cloud. So in that the files will be encrypted and uploaded to cloud. This comes under the double encryption. A systematic review is a means of evaluating and understanding all available research relevant to a particular research question or phenomenon of interest. It will provide better security to the cloud. the previous security issues in cloud computing but this proposed system aims to focus on the encryption methods used to resolve the security issue of the data confidentiality in cloud environment. And here we proposed another new concept that is key aggregation. In that system, provide more security than existing system. If you want, upload any data file images, audio, video in the cloud as well as in encrypted format and you can download anywhere no restriction for there. We have provided the facilities for the user to upload big size of the data file. When user upload the file then file is stored in encrypted form that mean file data is not human readable form. The particular file download then you select that file then automatic request go to the file owner when owner allow for the file access the generate key for download the file.

In proposed system, we have to implement key aggregation that is used to generate only one key for download the data. Key aggregation is used in our system. when any user request for download multiple file then all file owner to provide thier key and to access these all key generate only one small key in the form of OTD which comes on users mobile in the form of messages to the user that used to download the file. This system is better than existing system because we have to implement the additional concept is OTD (one time download). OTD is valid for only one time user can download the file. In proposed system implement one more concept that when the user request to any file in the cloud then generate notification in the form of OTD message to the file owner mobile or email. There is no required to go in online for received notification. If permission is given to the user then that user safely download and use it. Any user required any data then that user necessary to first register on our site and then access of the data.

III. ARCHITECTURE

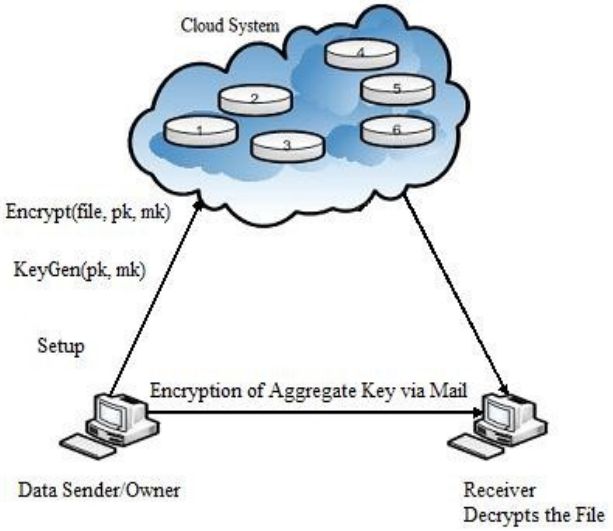

Figure 1. Double Encryption

In the architecture for double encryption and key aggregation on virtual cloud there is double encryption. In above fig.1 it shows the double encryption concept. Here in these double encryption users can directly select the file and uploaded it on the virtual cloud. In these phase the internal process is get started here in these proposed architecture we have to use any encryption decryption algorithms by which the system can easily encrypt the file and stored it over cloud. By the time of user when need the file again the he can just simply download the file but internally in the architecture there is a process of decryption. It is generally happened.

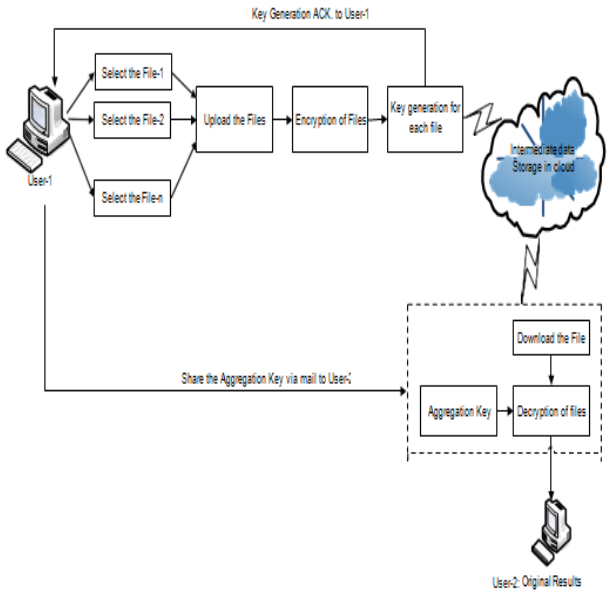

Figure 2. double encryption and key aggregation

Here again in the architecture the above fig.2 shows the key aggregation concept here in these multiple users can upload multiple files the files gets uploaded in the cloud. When any user required the file of another user. Then it just sends the request to particular users respectively. When the file owners can allow using then the key of multiple files get aggregated to one key in the form of OTD which comes on users mobile. And the user can use the OTD for download file.

IV. WORKING

The proposed system is very efficient as it is going to store as well as maintaining all data securely in the cloud.

This will providing the access the data anywhere any file one time is to upload then any user can access and use it this is more benefit for the user. In this system there is a database to store the record of that user to download or access any content then it is compulsory to register and login thier account in our website.

After creating account user can view all data files that are stored in cloud and it can be able to upload delete or download the file. In that what type of request enerated is depend on the user.

System will consider it as an input and apply algorithm to server side to encryption and decryption of the original data when the upload or download the process.

The algorithm generates an output, which will be readable, or non-readable form, which is benefit for the user. When any unwanted user can access file from the cloud then it can't readable form. All stored data on the cloud is encrypted form and this encrypt key available on the file owner.

The algorithm require Double Encryption and Key Aggregation which can be done by

- DES (Data Encryption Standered)

This System is work on the basis of following ways:

1. Any user first registers on site. After they login the account in our site.
2. After login into account user can directly perform operations on files such as upload file, download files, delete files and sending the request for files to other users.
3. If users have to upload the file then browse the file and upload on the site.
4. If the user have to download the file then select file and send request to file owner for the download permission .if the permission is allow to the user can got the key in the form of OTD to the user for the downloading for the file.

V. ADVANTAGES

User upload file very efficiently and securely in encrypted form. For more security reason when user wants to download the file then generate OTD of that user mobile. OTD is used only one time download .If the file one time download then OTD is expire. In that system user can search data file in file name as well as file owner name.

Cost Savings, Reliability, Manageability
Flexibility Disaster recovery Security

VI. CONCLUSION

Cloud computing is latest development that provides easy access to high performance computing resources without installation of software. It provides many benefits for its users but it suffers with some security threats. Security of data is one of the top list

impediments in the growth of this latest technology. In this study we provide a double encryption and key aggregation on virtual cloud. It aims for fixing the security related issues and provides reliability to the user.

VII. FUTURE SCOPE

The double encryption and key aggregation can support to its users to uploaded file can be downloaded anytime with having future scope. This mechanism can be having improved security with its file content and user can use it reliably. The OTD generation is the revolutionary concept used for downloading the uploaded files in cloud. And the owner of file can having total control over its file and he can gave file access to user based on its request.

Key aggregation is now used with this project. The leak of key concept is minimized with these projects. The OTD can be applied for only particular file and it will be for one time only.

VIII. REFERENCES

[1]. A. Sahai and B. Waters. Fuzzy identity based encryption. In EUROCRYPT, pages 457473, 2005.

[2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data," in New York, NY, USA: ACM, 2006.

[3]. J. Bettencourt, A. Sahai, and B. Waters, Cipher text-policy attribute based encryption," in Security and Privacy, 2007. IEEE Symposium.

[4]. L. Cheung and C. Newport, Provably secure cipher text policy abe, in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456465.

[5]. B. Waters, Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Public Key Cryptography PKC 2011. Springer, 2011, pp. 5370.

[6]. J. Li, G. Zhao, X. Chen, D. Xie, C. Rong, W. Li, L. Tang, and Y. Tang, Fine-grained data access control systems with user accountability in cloud computing," in IEEE Second International Conference on, 2010

[7]. C. Wang, X. Liu, and W. Li, Implementing a personal health record cloud platform using cipher text-policy attribute-based encryption," in 4th International Conference on, 2012, pp. 8-14.

[8]. S. Yu, C.Wang, K. Ren, and W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE, 2010.

[9]. S. Yu, C. Wang, K. Ren, W. Lou: Attribute based data sharing with attribute revocation. In: ASIACCS (2010).

[10]. Z. Wan, J. Liu, R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 5]